The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/11/2012

SUBJECT:

Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (MS12-081)

OVERVIEW:

A vulnerability has been discovered in the Windows that could allow for remote code execution. This vulnerability could be exploited by creating a specially file or folder that is located on the local system, network share, or downloaded from an external source. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the affected user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A remote code execution vulnerability exists in the way that Microsoft Windows parses file names. Given a special crafted file or folder, upon enumeration, could corrupt memory in such a way that allows an attacker to load arbitrary code and execute it within the privilege context of the current logged in user.

An attacker could exploit the vulnerability in the following scenarios:

- An attacker could store a specially named file or folder on a network share, UNC path, WebDav directory and encourage a user to visit that directory.
- An attacker could e-mail a specially named file as an attachment to a user and encourage them to browse to that attachments location.
- An attacker could host a specially crafted file on a website and encourage a user to download that file and browse to its location on the file system.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Discourage users from downloading and opening suspicious attachments and files from untrusted sources.
- Discourage users from visiting links to suspicious websites.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms12-081

SecurityFocus:

http://www.securityfocus.com/bid/56443

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4774